REMARKS

In the Official Action mailed on **13 June 2005**, the Examiner reviewed claims 1-11, 13-29, 31-47, and 49-54. Claims 1, 4, 5, 8, 9, 13, 15, 16, 18, 19, 22, 23, 26, 27, 31, 33, 34, 36, 37, 40, 41, 44, 45, 49, 51, 52, and 54 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bruce Schneier (*Applied Cryptography 2nd Edition*, Oct. 1995, John Wiley & Sons Pub. pages 43-57, hereinafter "Schneier") in view of Medvinski et al (*Public Key Utilizing Tickets for Application Servers*, hereinafter "Medvinski") and Kohl et al (*The Kerberos Network Authentication Service, Network Working Group Request For Comments (RFC) 1510*, Sept. 1993, hereinafter "Kohl"). Claims 14, 17, 32, 35, 50, and 53 were rejected as being unpatentable over Schneier in view of Medvinski and Official Notice (hereinafter "ON"). Claims 2, 3, 6, 7, 10, 11, 20, 21, 24, 25, 28, 29, 38, 39, 42, 43, 46, and 47 were rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Medvinski and Sirbu et al (*Public Key Based Ticket Granting service in Kerberos*, hereinafter "Sirbu") and ON.

Rejections under 35 U.S.C. §103(a)

Independent claims 1, 19, and 37 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Medvinski and Kohl.

Applicant respectfully points out that both Medvinski and Kohl teach away from the present invention.

Kohl describes the Kerberos network authentication system, which provides a means of verifying the identities of principals on an open network. Kerberos allows a client to obtain a "ticket" from a key distribution center (KDC) which enables the client to (a) authenticate itself to a server and (b) initiate a secure session with the server. Note that Kerberos uses a **long-term secret key** which is shared between the KDC and the server to seal the ticket (see Kohl, section 1.3, definitions for "secret key" and "ticket").

Before a client can obtain a ticket for a server, the client and server must authenticate themselves with the KDC. PKINIT extends Kerberos so that clients and servers can use public key cryptography to authenticate themselves with the KDC. But, after authentication, a *"client can proceed in a normal fashion, using the conventional Kerberos ticket"* (see Medvinski, last paragraph of section 4). Furthermore, Medvinski describes *"how, **without any modification**, the PKINIT specification may be used to implement the ideas introduced in PKDA"* (see Medvinski, Abstract). In other words, Medvinski uses a **long-term secret key** to generate a ticket because PKINIT uses the conventional Kerberos ticket which uses a long-term secret key.

In contrast, the present invention is specifically directed towards using a **temporary secret key** to generate a ticket. In particular, the present invention creates a ticket by *"encrypting an identifier for the client and the session key with the temporary secret key"* (see page 4, lines 24-25).

Using a temporary secret key to generate a ticket is very advantageous because it reduces vulnerability. Note that vulnerability is reduced because the temporary key will eventually become invalid after a specified time period (see page 9, lines 24-26). Furthermore, managing temporary secret keys is not obvious because it involves the complex operations shown in FIG. 2.

Accordingly, Applicant has amended independent claims 1, 19, and 37 to clarify that invalidating the temporary secret key after a specified time reduces the vulnerability of the KDC. These amendments find support on page 9, lines 24-26.

Hence, Applicant respectfully submits that independent claims 1, 19, and 37 as presently amended are in condition for allowance. Applicant also submits that claims 2-11 and 13-18, which depend upon claim 1, claims 21-29 and 31-36, which depend upon claim 19, and claims 38-47 and 49-54, which depend upon claim 37, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By   _A. Richard Park_

A. Richard Park
Registration No. 41,241

Date: 9 August 2005

A. Richard Park
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95616
Tel: (530) 759-1661
FAX: (530) 759-1665